HPE Aruba Networking EdgeConnect Security Bulletin

This Security Bulletin covers Orchestrator Advanced Security Settings

2023-03-21

Version 1.0 – Initial Release

Contents

EdgeConnect Orchestrator Deployment Models

Orchestrator releases covered in this bulletin:

Orchestrator Model	Deployment Model	Affected Releases
Aruba EdgeConnect Enterprise Orchestrator	Self-hosted On Prem	**This Bulletin applies to all existing Orchestrator instances independent of release.**
	Self-hosted Public Cloud IaaS	
Aruba EdgeConnect Enterprise Orchestrator-as-a-Service (OaaS)	Enterprise, Single Tenant OaaS	
	Orchestrator-SP Tenant OaaS	
	Orchestrator Global Enterprise Tenant OaaS	

Security Settings for Orchestrator

Orchestrator Advanced Security Settings

Newly provisioned Orchestrators have the following default values for Advance Security Settings:

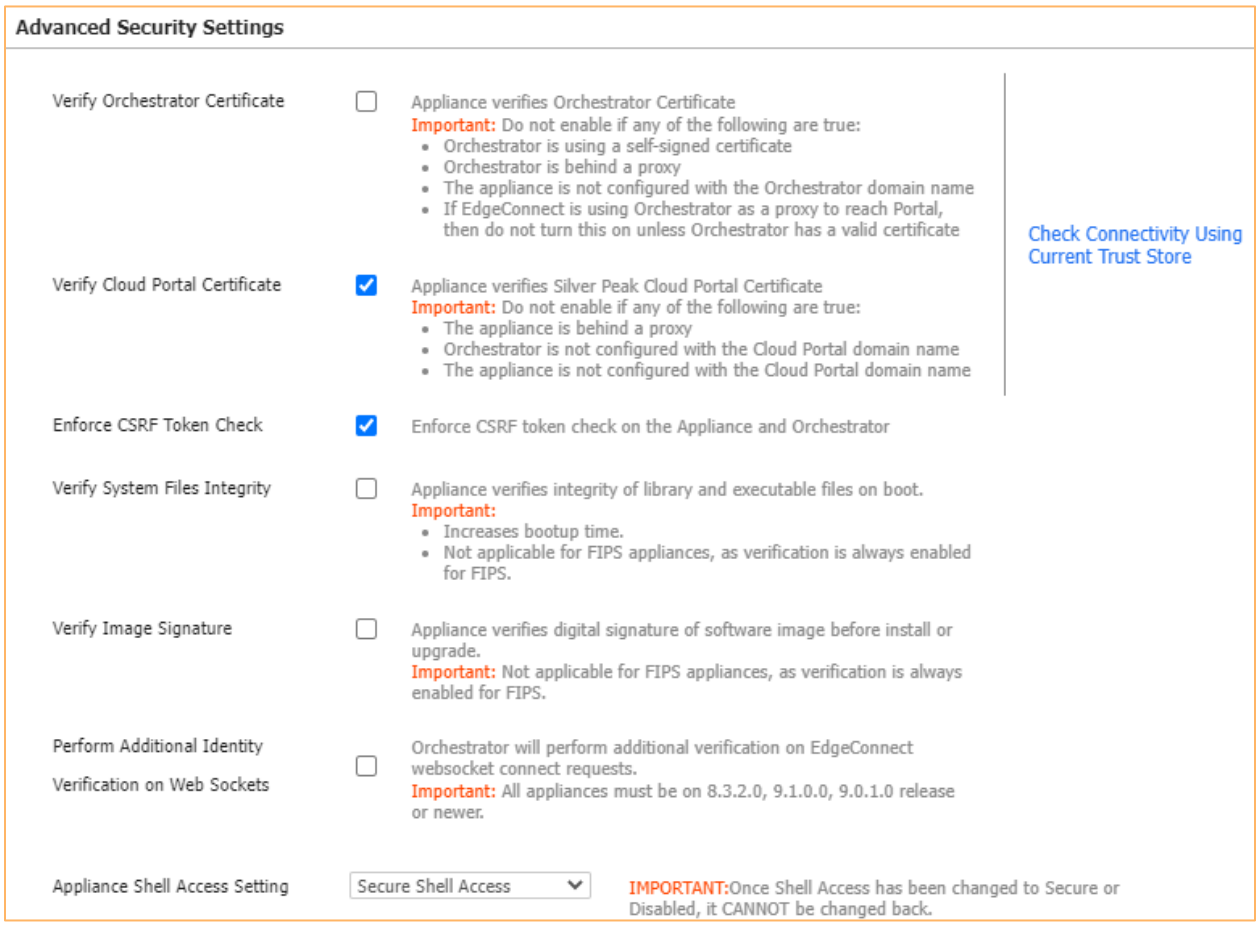
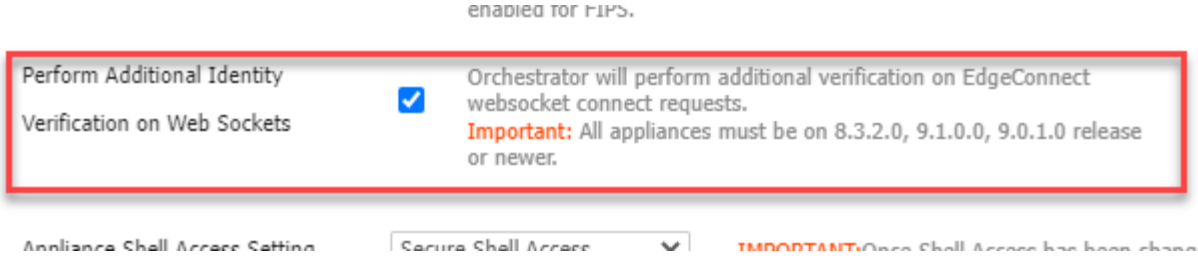


Figure 1 Orchestrator 9.x Advanced Security Settings - Default Values

The primary purpose of this security bulletin is to ensure customers have the “Perform Additional Identity Verification on Web Socket set as enabled.



If your EdgeConnect-only network is running ECOS version 8.3.2.0 or newer, the “Perform Additional Identity Verification on Web Sockets” option **must be enabled**. On future versions of Orchestrator, this option will be removed and will always be on.

Recommended Security Settings

The Advanced Security Settings menu provides controls for management plane security between Cloud Portal, Orchestrator, and EdgeConnect appliances. From a security hardening perspective, Aruba strongly recommends enabling all these settings. Starting with Release 9.0, newly instantiated Orchestrators default to Secure Shell Access.

To enable these settings:

1. Navigate to Configuration > Overlays & Security > Security > Advanced Security Settings.
2. Select all check boxes in the Advanced Security Settings window.
3. Enable the Advanced Security Settings as shown below.
4. Click **Save**.

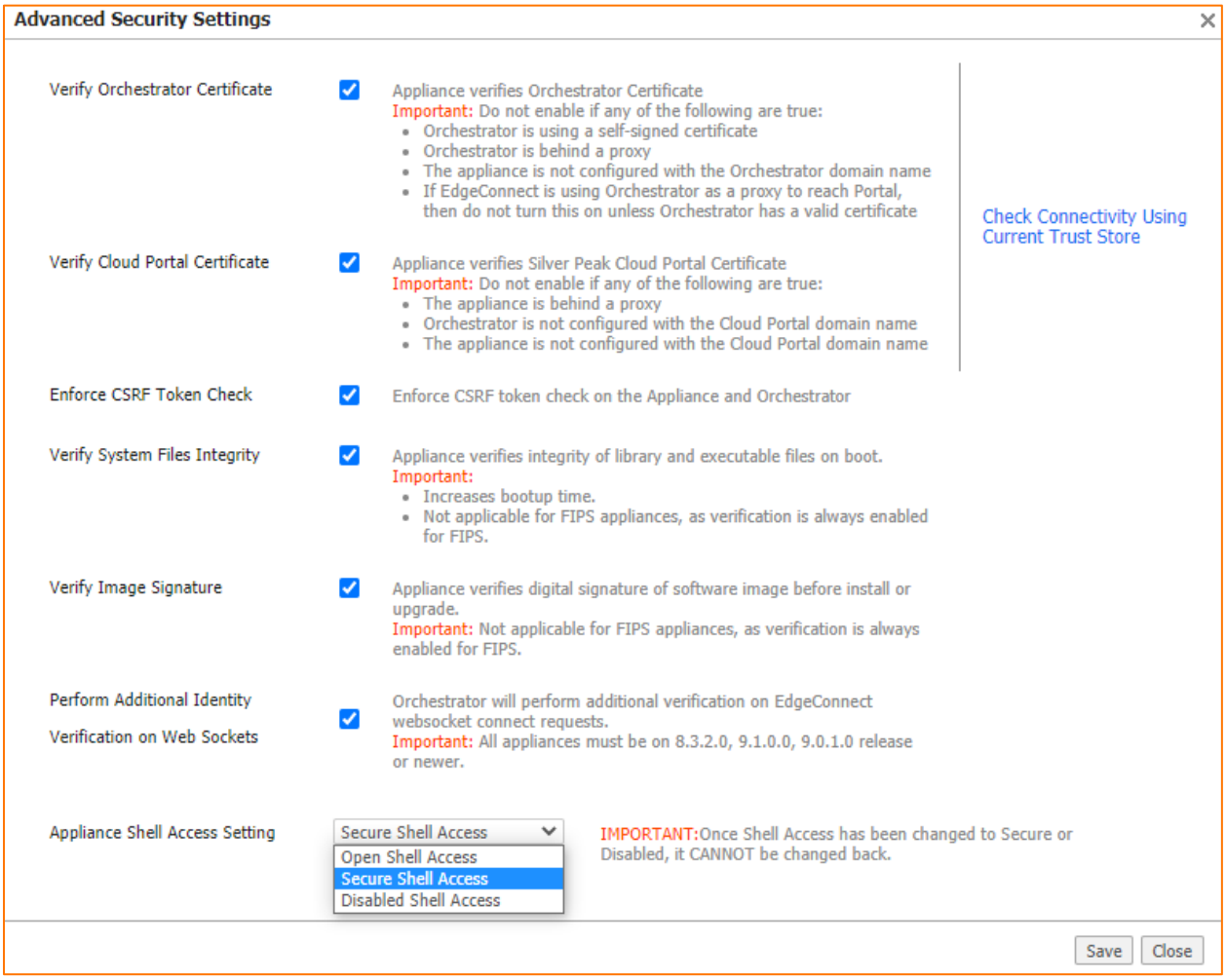


Figure 2 Orchestrator Advanced Security Settings – Aruba Recommendation

NOTE: Not all of these are set by default for new Orchestrators. The administrator must ensure that these settings are ALL enabled (Aruba recommendation).

For more details on each setting, see Table 1.

Table 1: Orchestrator Advanced Security Settings

Setting	Description
Verify Orchestrator Certificate	• EdgeConnect appliances verify the Orchestrator Certificate. If a customer-managed Orchestrator is not configured with a proper certificate, this cannot be enabled. Silver Peak hosted Orchestrator-as-a-Service and Cloud Portal are configured with properly signed certificates. Aruba recommends this setting be enabled. If there is an SSL proxy between the EdgeConnect and Orchestrator, there are additional steps to add the CA certificates to the EdgeConnect trust store to trust the SSL proxy instead.

Setting	Description
Verify Cloud Portal Certificate	• EdgeConnect appliances verify the Aruba Cloud Portal Certificate. Aruba recommends this setting be enabled. If there is an SSL proxy between the EdgeConnect and CloudPortal, there are additional steps to add the CA certificates to the EdgeConnect trust store to trust the SSL proxy instead.
Enforce CSRF Token Check	Enforce CSRF token check on the appliance and Orchestrator. Aruba recommends this setting always be enabled.
Verify System Files Integrity	Appliance verifies the integrity of library and executable files on boot. Aruba recommends this setting be enabled. **NOTES:** • When enabled, this setting increases bootup time. • Appliances with FIPS mode enabled always perform system files integrity check.
Verify Image Signature	Appliance verifies the digital signature of the software image before install or upgrade. Aruba recommends this setting be enabled. **NOTE:** Appliances with FIPS mode enabled always verify image signature.
Perform Additional Identity Verification on Web Sockets	Orchestrator performs additional verification on EdgeConnect WebSocket connection requests. ECOS uses account name and account key to authenticate with Orchestrator. EdgeConnect creates a signed token using its account key and attaches it to the X-AUTH-TOKEN HTTP header of the WebSocket request. For secure operations Aruba strongly recommends that the Additional Identity Verification check always be enabled.
Appliance Shell Access Setting	• **Open Shell Access:** ECOS admin users have full access to the underlying Linux shell. This is the case for Orchestrators prior to Release 9.0 and will remain the case after Orchestrator is upgraded to Release 9.0 or later. This setting is NOT recommended. For customers with Orchestrators that were upgraded from releases prior to R9.0, Aruba advises changing this setting to **Secure Shell Access**. • **Secure Shell Access:** ECOS admin users need a token granted by Aruba Technical Support to access the underlying Linux shell for troubleshooting. This is the default value for Orchestrators instantiated with Release 9.0 or later. At a minimum, Aruba recommends this setting. • **Disabled Shell Access:** Linux shell is permanently disabled. **NOTES:** • Appliances with FIPS mode enabled completely disable shell access independent of this setting. • After shell access has been changed to Secure or Disabled, it CANNOT be changed back.

EdgeConnect and/or VX Network Deployments

Network Model	Action
EdgeConnect-only deployments	Set Orchestration Advanced Security Settings per recommendations above
EdgeConnect, VX mixed deployment	Orchestrator must not be accessible through any Internet Connection. Orchestrator must be completely isolated on a private network. A software upgrade to enhance the default security options will be forthcoming – to be announced.
VX-only deployments	Orchestrator must not be accessible through any Internet Connection. Orchestrator must be completely isolated on a private network. A software upgrade to enhance the default security options will be forthcoming – to be announced.

End of Document

Hewlett Packard Enterprise